

nology, including timelines, to develop standards for post-quantum cryptography, including any Federal Information Processing Standards developed under chapter 35 of title 44, as well as standards developed through voluntary, consensus standards bodies such as the International Organization for Standardization.

**(2) Report on migration to post-quantum cryptography in information technology**

Not later than 1 year after the date on which the Director of OMB issues guidance under subsection (c)(2), and thereafter until the date that is 5 years after the date on which post-quantum cryptographic standards are issued, the Director of OMB, in coordination with the National Cyber Director and in consultation with the Director of CISA, shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives, with the report submitted pursuant to section 3553(c) of title 44, a report on the progress of agencies in adopting post-quantum cryptography standards.

(Pub. L. 117–260, § 4, Dec. 21, 2022, 136 Stat. 2390.)

**Editorial Notes**

**CODIFICATION**

Section was enacted as part of the Quantum Computing Cybersecurity Preparedness Act, and not as part of the Cybersecurity Act of 2015 which comprises this chapter.

**Statutory Notes and Related Subsidiaries**

**FINDINGS; SENSE OF CONGRESS**

Pub. L. 117–260, § 2, Dec. 21, 2022, 136 Stat. 2389, provided that:

“(a) FINDINGS.—Congress finds the following:

“(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.

“(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide cybersecurity.

“(3) Quantum computers might one day have the ability to push computational boundaries, allowing us to solve problems that have been intractable thus far, such as integer factorization, which is important for encryption.

“(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

“(b) SENSE OF CONGRESS.—It is the sense of Congress that—

“(1) a strategy for the migration of information technology of the Federal Government to post-quantum cryptography is needed; and

“(2) the governmentwide and industrywide approach to post-quantum cryptography should prioritize developing applications, hardware intellectual property, and software that can be easily updated to support cryptographic agility.”

**EXEMPTION OF NATIONAL SECURITY SYSTEMS**

Pub. L. 117–260, § 5, Dec. 21, 2022, 136 Stat. 2392, provided that: “This Act [see Short Title of 2022 Amendment note set out under section 1500 of this title] shall not apply to any national security system.”

**DEFINITIONS**

Pub. L. 117–260, § 3, Dec. 21, 2022, 136 Stat. 2389, provided that: “In this Act [see Short Title of 2022 Amendment note set out under section 1500 of this title]:

“(1) AGENCY.—The term ‘agency’—

“(A) means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

“(B) does not include—

“(i) the Government Accountability Office; or

“(ii) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions.

“(2) CLASSICAL COMPUTER.—The term ‘classical computer’ means a device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed and encodes information in binary bits that can either be 0s or 1s.

“(3) DIRECTOR OF CISA.—The term ‘Director of CISA’ means the Director of the Cybersecurity and Infrastructure Security Agency.

“(4) DIRECTOR OF NIST.—The term ‘Director of NIST’ means the Director of the National Institute of Standards and Technology.

“(5) DIRECTOR OF OMB.—The term ‘Director of OMB’ means the Director of the Office of Management and Budget.

“(6) INFORMATION TECHNOLOGY.—The term ‘information technology’ has the meaning given the term in section 3502 of title 44, United States Code.

“(7) NATIONAL SECURITY SYSTEM.—The term ‘national security system’ has the meaning given the term in section 3552 of title 44, United States Code.

“(8) POST-QUANTUM CRYPTOGRAPHY.—The term ‘post-quantum cryptography’ means those cryptographic algorithms or methods that are assessed not to be specifically vulnerable to attack by either a quantum computer or classical computer.

“(9) QUANTUM COMPUTER.—The term ‘quantum computer’ means a computer that uses the collective properties of quantum states, such as superposition, interference, and entanglement, to perform calculations.”

**SUBCHAPTER III—OTHER CYBER MATTERS**

**§ 1531. Apprehension and prosecution of international cyber criminals**

**(a) International cyber criminal defined**

In this section, the term “international cyber criminal” means an individual—

(1) who is believed to have committed a cybercrime or intellectual property crime against the interests of the United States or the citizens of the United States; and

(2) for whom—

(A) an arrest warrant has been issued by a judge in the United States; or

(B) an international wanted notice (commonly referred to as a “Red Notice”) has been circulated by Interpol.

**(b) Consultations for noncooperation**

The Secretary of State, or designee, shall consult with the appropriate government official of each country from which extradition is not likely due to the lack of an extradition treaty with the United States or other reasons, in which one or more international cyber criminals are physically present, to determine what actions the government of such country has taken—

(1) to apprehend and prosecute such criminals; and

(2) to prevent such criminals from carrying out cybercrimes or intellectual property crimes against the interests of the United States or its citizens.

**(c) Annual report**

**(1) In general**

The Secretary of State shall submit to the appropriate congressional committees an annual report that includes—

(A) the number of international cyber criminals located in other countries, disaggregated by country, and indicating from which countries extradition is not likely due to the lack of an extradition treaty with the United States or other reasons;

(B) the nature and number of significant discussions by an official of the Department of State on ways to thwart or prosecute international cyber criminals with an official of another country, including the name of each such country; and

(C) for each international cyber criminal who was extradited to the United States during the most recently completed calendar year—

(i) his or her name;

(ii) the crimes for which he or she was charged;

(iii) his or her previous country of residence; and

(iv) the country from which he or she was extradited into the United States.

**(2) Form**

The report required by this subsection shall be in unclassified form to the maximum extent possible, but may include a classified annex.

**(3) Appropriate congressional committees**

For purposes of this subsection, the term “appropriate congressional committees” means—

(A) the Committee on Foreign Relations, the Committee on Appropriations, the Committee on Homeland Security and Governmental Affairs, the Committee on Banking, Housing, and Urban Affairs, the Select Committee on Intelligence, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Foreign Affairs, the Committee on Appropriations, the Committee on Homeland Security, the Committee on Financial Services, the Permanent Select Committee on Intelligence, and the Committee on the Judiciary of the House of Representatives.

(Pub. L. 114–113, div. N, title IV, § 403, Dec. 18, 2015, 129 Stat. 2979.)

**§ 1532. Enhancement of emergency services**

**(a) Collection of data**

Not later than 90 days after December 18, 2015, the Secretary of Homeland Security, acting through the center established under section 659 of this title, in coordination with appropriate Federal entities and the Assistant Director for Emergency Communications, shall establish a process by which a Statewide Interoperability Coordinator may report data on any

cybersecurity risk or incident involving any information system or network used by emergency response providers (as defined in section 101 of this title) within the State.

**(b) Analysis of data**

Not later than 1 year after December 18, 2015, the Secretary of Homeland Security, acting through the Director of the National Cybersecurity and Communications Integration Center, in coordination with appropriate entities and the Assistant Director for Emergency Communications, and in consultation with the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers.

**(c) Best practices**

**(1) In general**

Using the results of the integration and analysis conducted under subsection (b), and any other relevant information, the Director of the National Institute of Standards and Technology shall, on an ongoing basis, facilitate and support the development of methods for reducing cybersecurity risks to emergency response providers using the process described in section 272(e) of title 15.

**(2) Report**

The Director of the National Institute of Standards and Technology shall submit to Congress a report on the result of the activities of the Director under paragraph (1), including any methods developed by the Director under such paragraph, and shall make such report publicly available on the website of the National Institute of Standards and Technology.

**(d) Rule of construction**

Nothing in this section shall be construed to—

(1) require a State to report data under subsection (a); or

(2) require a non-Federal entity (as defined in section 1501 of this title) to—

(A) adopt a recommended measure developed under subsection (b); or

(B) follow the result of the activities carried out under subsection (c), including any methods developed under such subsection.

(Pub. L. 114–113, div. N, title IV, § 404, Dec. 18, 2015, 129 Stat. 2980; Pub. L. 115–278, § 2(h)(1)(H), Nov. 16, 2018, 132 Stat. 4183.)

**Editorial Notes**

**AMENDMENTS**

2018—Subsec. (a). Pub. L. 115–278, § 2(h)(1)(H), substituted “section 659 of this title” for “section 148 of this title, as redesignated by section 223(a)(3) of this division,” and “Assistant Director for Emergency Communications” for “Director for Emergency Communications”.

Subsec. (b). Pub. L. 115–278, § 2(h)(1)(H)(ii), substituted “Assistant Director for Emergency Communications” for “Director for Emergency Communications”.

**Statutory Notes and Related Subsidiaries****CHANGE OF NAME**

Reference to the Assistant Director for Emergency Communications deemed to be a reference to the Executive Assistant Director for Emergency Communications, see section 571(g) of this title, enacted Jan. 1, 2021.

**§ 1533. Improving cybersecurity in the health care industry****(a) Definitions**

In this section:

**(1) Appropriate congressional committees**

The term “appropriate congressional committees” means—

(A) the Committee on Health, Education, Labor, and Pensions, the Committee on Homeland Security and Governmental Affairs, and the Select Committee on Intelligence of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Homeland Security, and the Permanent Select Committee on Intelligence of the House of Representatives.

**(2) Business associate**

The term “business associate” has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

**(3) Covered entity**

The term “covered entity” has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

**(4) Cybersecurity threat; cyber threat indicator; defensive measure; Federal entity; non-Federal entity; private entity**

The terms “cybersecurity threat”, “cyber threat indicator”, “defensive measure”, “Federal entity”, “non-Federal entity”, and “private entity” have the meanings given such terms in section 1501 of this title.

**(5) Health care clearinghouse; health care provider; health plan**

The terms “health care clearinghouse”, “health care provider”, and “health plan” have the meanings given such terms in section 160.103 of title 45, Code of Federal Regulations (as in effect on the day before December 18, 2015).

**(6) Health care industry stakeholder**

The term “health care industry stakeholder” means any—

(A) health plan, health care clearinghouse, or health care provider;

(B) advocate for patients or consumers;

(C) pharmacist;

(D) developer or vendor of health information technology;

(E) laboratory;

(F) pharmaceutical or medical device manufacturer; or

(G) additional stakeholder the Secretary determines necessary for purposes of subsection (b)(1), (c)(1), (c)(3), or (d)(1).

**(7) Secretary**

The term “Secretary” means the Secretary of Health and Human Services.

**(b) Report****(1) In general**

Not later than 1 year after December 18, 2015, the Secretary shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats.

**(2) Contents of report**

With respect to the internal response of the Department of Health and Human Services to emerging cybersecurity threats, the report under paragraph (1) shall include—

(A) a clear statement of the official within the Department of Health and Human Services to be responsible for leading and coordinating efforts of the Department regarding cybersecurity threats in the health care industry; and

(B) a plan from each relevant operating division and subdivision of the Department of Health and Human Services on how such division or subdivision will address cybersecurity threats in the health care industry, including a clear delineation of how each such division or subdivision will divide responsibility among the personnel of such division or subdivision and communicate with other such divisions and subdivisions regarding efforts to address such threats.

**(c) Health care industry cybersecurity task force****(1) In general**

Not later than 90 days after December 18, 2015, the Secretary, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security, shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the Secretary determines appropriate to establish a task force to—

(A) analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries;

(B) analyze challenges and barriers private entities (excluding any State, tribal, or local government) in the health care industry face securing themselves against cyber attacks;

(C) review challenges that covered entities and business associates face in securing networked medical devices and other software or systems that connect to an electronic health record;

(D) provide the Secretary with information to disseminate to health care industry stakeholders of all sizes for purposes of improving their preparedness for, and response to, cybersecurity threats affecting the health care industry;

(E) establish a plan for implementing subchapter I of this chapter, so that the Federal

Government and health care industry stakeholders may in real time, share actionable cyber threat indicators and defensive measures; and

(F) report to the appropriate congressional committees on the findings and recommendations of the task force regarding carrying out subparagraphs (A) through (E).

## **(2) Termination**

The task force established under this subsection shall terminate on the date that is 1 year after the date on which such task force is established.

## **(3) Dissemination**

Not later than 60 days after the termination of the task force established under this subsection, the Secretary shall disseminate the information described in paragraph (1)(D) to health care industry stakeholders in accordance with such paragraph.

## **(d) Aligning health care industry security approaches**

### **(1) In general**

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that—

(A) serve as a resource for cost-effectively reducing cybersecurity risks for a range of health care organizations;

(B) support voluntary adoption and implementation efforts to improve safeguards to address cybersecurity threats;

(C) are consistent with—

(i) the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 272(c)(15) of title 15;

(ii) the security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and

(iii) the provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and

(D) are updated on a regular basis and applicable to a range of health care organizations.

## **(2) Limitation**

Nothing in this subsection shall be interpreted as granting the Secretary authority to—

(A) provide for audits to ensure that health care organizations are in compliance with this subsection; or

(B) mandate, direct, or condition the award of any Federal grant, contract, or purchase, on compliance with this subsection.

## **(3) No liability for nonparticipation**

Nothing in this section shall be construed to subject a health care industry stakeholder to liability for choosing not to engage in the voluntary activities authorized or guidelines developed under this subsection.

## **(e) Incorporating ongoing activities**

In carrying out the activities under this section, the Secretary may incorporate activities that are ongoing as of the day before December 18, 2015 and that are consistent with the objectives of this section.

## **(f) Rule of construction**

Nothing in this section shall be construed to limit the antitrust exemption under section 1503(e) of this title or the protection from liability under section 1505 of this title.

(Pub. L. 114-113, div. N, title IV, § 405, Dec. 18, 2015, 129 Stat. 2981.)

## **Editorial Notes**

### **REFERENCES IN TEXT**

Section 264(c) of the Health Insurance Portability and Accountability Act of 1996, referred to subsec. (d)(1)(C)(ii), is section 264(c) of Pub. L. 104-191, which is set out as a note under section 1320d-2 of Title 42, The Public Health and Welfare.

The Health Information Technology for Economic and Clinical Health Act, referred to in subsec. (d)(1)(C)(iii), is title XIII of div. A and title IV of div. B of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 226, 467, also known as the HITECH Act. For complete classification of this Act to the Code, see Short Title of 2009 Amendment note set out under section 201 of Title 42, The Public Health and Welfare, and Tables.

## **§ 1534. Cybercrime**

Subject to the availability of appropriations, and in accordance with the comparable level of the General Schedule, the Attorney General and the Secretary of Homeland Security shall provide incentive pay, in an amount that is not more than 25 percent of the basic pay of the individual, to an individual appointed to a position in the Department of Justice (including the Federal Bureau of Investigation) or the Department of Homeland Security (including positions in Homeland Security Investigations), respectively, requiring significant cyber skills, including to aid in—

(1) the protection of trafficking victims;

(2) the prevention of trafficking in persons; or

(3) the prosecution of technology-facilitated crimes against children by buyers or traffickers in persons.

(Pub. L. 117-347, title IV, § 401, Jan. 5, 2023, 136 Stat. 6207.)

## **Editorial Notes**

### **REFERENCES IN TEXT**

The General Schedule, referred to in text, is set out under section 5332 of Title 5, Government Organization and Employees.

### **CODIFICATION**

Section was enacted as part of the Abolish Trafficking Reauthorization Act of 2022, and not as part of

the Cybersecurity Act of 2015 which comprises this chapter.